Data storage

Data is stored in the application directory. Which is found like this:

```
/var/mobile/Containers/Data/Application/$APP_ID/
```

In order to find the APP_ID you can do the following:

First you list all applications, and identify your application:

```
ipainstaller -l
```

Then search all directories for that name

```
find ./ -iname PACKAGE-Name
```

References: http://www.securitylearn.net/2013/04/15/penetration-testing-of-iphone-applications-part-4/

Check that snapshots of sensitive data is not stored

Whenever a user backgrounds an application a snaopshot i taken.

You can find them here:

```
/private/var/mobile/Containers/Data/Application/<GUID>/Library/Caches/Snapshots
```

In order to view the file you can use this script to convert it to PNG: https://github.com/ydkhatri/MacForensics/blob/master/IOS_KTX_TO_PNG/ios_ktx2png.py

Check for secrets or sensitive information in plist files

`plist` is a structured binary formatted file. It can contain interesting data. You can't read plist files with cat, put you can read them with plistutils

```
sudo aptitude install libplist-utils
plistutil -i file.plist
```

The files are usually stored in `[Application's Home Directory]/documents/preferences`. The files are usually used to store applications and configurations. But they can be used to store session information, passwords or whatever.

Authorisation and authention can be decided based on entries in a plist.

Find plist the following way:

```
find ./ -iname *plist
```

However, note that the plist fileending.

Check for other sensitive data in documents

Browse around and see if they are storing sensitive stuff here.

Check for sensitive data in sqlite databases

```
find ./ -iname *sqlite -o -iname *db -o -iname *sqlitedb
```

Check for sensitive data in keyboard cache

Check that sensitive data is not persistent in keychain

Unintended data leaks

Check for Firebase access control

Look for a string looking like this `somethingsomething.firebaseio.com`. Check if you can access sensitive data in: `somethingsomething.firebaseio.com/.json`